MICROSOFT PUBLIC SECTOR CLOUD DESIGN

Azure Services in the Swiss Public Sector

Version 1.4

Microsoft

Related documents

Document name	
Microsoft Public Sector Cloud Design	
Document: Cloud Governance & Security in the Swiss Public Sector V1.4	
Identification: Governance and Security Guideline Swiss Public Sector_V1.4	
Azure Blueprints for Public Sector (ISO 27001)	Microsoft Docs

Microsoft

Contents

Tables

Figures

Disclaimer

This document covers the questions often asked by our customers on the use of cloud computing solutions. It should enable you to better understand the technical and legal contexts involved in the use of a cloud computing solution. This document does not include a specific examination of an individual legal situation. You will have to seek separate legal advice to obtain an individual and definitive legal assessment on the acceptability of the use of Microsoft Cloud solutions specific to your situation.

1 INTRODUCTION TO MICROSOFT PUBLIC SECTOR CLOUD DESIGN – MPSD

The use of cloud solutions is now widespread and, given the growing number of affordable offers, is also becoming increasingly popular with public authorities. The clear benefits come with challenges that public authorities need to consider: the data resides with the cloud provider but remains under the control of the authorities. Data processing is said to be "outsourced" to the cloud provider. To ensure control of the outsourced data processing, public authorities need to consider the conditions offered by the cloud provider, particularly in terms of information security.

The question is then what help Microsoft, as cloud service provider, can offer its public sector customers who choose to use its online services. Public authority customers should be aware of the resulting risks and the contractual, organizational and technical means that Microsoft deploys to ensure the security of its online services.

1.1 DATA CONTROL AS THE FOCUS OF CONCERNS

In cloud solutions, the data is processed not on the customer's own computers or local servers but on the technical infrastructure of specialized third-party providers, such as Microsoft. Legally, such data processing by third parties is permissible, in principle, provided that the compliance requirements specific to each case are complied with and, above all, that the data controller "retains control."

Control in this context implies, on one hand, the guarantee by technical, organizational and contractual measures that only authorized persons have access to the data, and that the obligations provided for by data protection law (security measures, reporting obligations, compliance with processing principles, etc.) are satisfied. It is important to ensure that third parties authorized to access the data do not make unauthorized use of such data and actually and definitively delete it at the request of the data controller. In the case of cloud solutions, this control requirement also implies the possibility of re-transferring, within a reasonable period and effort, the outsourced data to its own or other infrastructure.

The concrete requirements to be met vary depending on the circumstances and nature of the data. These requirements are particularly higher when data is transmitted unencrypted to the third-party provider (the transmission of data to Azure services is generally always encrypted) or when its use by an unauthorized third party risks having a strong impact on the data subjects (secret official documents, for example).

The "control" requirement is not explicitly stated in any statute or general statutory provision. However, all acts of federal law and cantonal legislation relating to the right to information implicitly seek to establish the requirements of control over information. If we reduce the various applicable legal standards to their essentials, a control obligation emerges to some extent as the central theme.

Similarly, the instruments used to exercise and guarantee data control in on-premise IT infrastructures and cloud solutions are fundamentally similar since they always consist of technical, organizational and contractual measures.

2 THE LEGAL CHALLENGES OF CLOUD DESIGN

2.1 PRIMARY INFORMATION

Despite the "Cloud First" principle already included in the "Swiss Cloud Computing Strategy" adopted almost ten years ago, public authorities still show a certain reluctance that can probably be attributed to the mistrust inspired by cloud solutions. Eight years after the adoption of the "Cloud First" principle, however, there is still (or already) a question in the 2020 Cloud Strategy of a **paradigm shift in favor of "Cloud First"** (Cloud Strategy 2020)[1].

Mistrust can be seen at all federated levels of authority, namely, within the federal, cantonal and municipal authorities. While federal authorities are primarily subject to the data protection law and other federal acts, cantonal and communal authorities must not only comply with the data protection law but also, where appropriate, other acts of their canton. What applies, however, to public authority entities at all levels is their official secrecy and criminal liability in the event of a violation of this secrecy.

2.1.1 Cloud computing as de facto outsourcing

In cloud solutions, the data is processed not on the customer's own computers or local servers but on the technical infrastructure of specialized third-party providers, and its management is performed by external personnel. This is therefore a so-called outsourcing situation within the meaning of data protection legislation.

However, cloud solutions should be distinguished from traditional outsourcing solutions, which also constitute de facto outsourcing according to the applicable data protection provisions. In general, "classical" outsourcing refers to the case where a service provider manages operations on behalf of the customer in accordance with the customer's specific instructions and, as such, obtains access to the data that it can therefore view. In a cloud model, however, the customer receives a **standardized service**. The **individual nature** or **lack of individual nature** of the service relationship (at the technical and organizational level) is therefore a major criterion that differentiates cloud computing from traditional outsourcing. The transition between these two forms is nevertheless fluid.

2.1.2 Offshore

If, in the cloud solution context, personal data is processed in countries with a lower level of data protection than that of Switzerland, the EU or the EEA (this is then a "lack of equivalence" in so-called "unsafe" foreign countries), the admissibility of this data processing will depend on compliance not only with the general requirement of control but with additional conditions as well (e.g. the existence of protective contractual measures, see also 4.15).

[1] https://www.newsd.admin.ch/newsd/message/attachments/64752.pdf

2.2 LEGAL PROVISIONS

2.2.1 General Information

Since the Confederation does not have general competence to legislate in the data protection domain, the cantons are, by virtue of their right to organize themselves, authorized to regulate the protection of personal data that are processed by the cantonal and communal public authorities. All of the cantons have adopted general data protection decrees. By defining the conditions and general principles of data processing applied by the cantonal and communal authorities as well as the rights of the data subjects, these decrees encapsulate the fundamental right to the protection of the person and the principles of the rule of law relating to the processing of personal data at the cantonal level. The involvement of cantonal public entities in private economic tenders does not fall within the exercise of sovereign functions or public tasks under cantonal law (especially for cantonal banks).

Legal provisions specific to the processing of data through subcontracting can be found in the Swiss Federal Act on Data Protection Act (FADP) and in most cantonal laws on data protection. This processing takes place when the responsible public entity entrusts the performance of data processing to a third party.

Some cantons have specific regulations on outsourcing conditions in the event of data processing operations entrusted to third parties (agreement in a written contract, specific regulations on subcontracting, etc.). However, most cantons do not promulgate rules that go beyond the requirements of the FADP.

In general, subcontracting is, in principle, permitted if there are no legal or contractual confidentiality obligations to the contrary and if compliance with data protection regulations is guaranteed. Federal and cantonal data protection legislation is based on a comparable basic principle here.

The public entity awarding the contract remains fundamentally responsible for data protection compliance and must take measures to ensure a sufficient level of data protection.

2.2.2 The most common guidelines

2.2.2.1 Contractual agreement

An outsourcing contract must be concluded with third parties who assume responsibility for the outsourced processing of data on behalf of a public authority (Microsoft, for example). This contract will regulate the guarantees of data protection, security compliance and the use of cloud services in the public law domain.

Depending on the canton, there are legal provisions regulating the content of the contract to be signed with the subcontractor. Some cantons also have "General Conditions" that must accompany contracts for the outsourcing of IT services or the processing of personal data.[2] It is fundamentally possible to deviate from these requirements in the interest of finding a suitable solution, especially when there are no compelling reasons arising from the legal situation to justify an unchanged application of these FADP or if, after examination, the requirements for the sufficient contractual regulation of data protection and data security are satisfactorily taken into account in the service provider's contracts.

Consistent with the nature of a "cloud" and its standardized offerings for all customers, Microsoft employs standard contracts that govern the use of cloud infrastructure. The consideration of individual constraints on a larger scale is difficult on this highly standardized IT infrastructure and must be clarified on a case-by-case basis, and Microsoft will always assist in this process.

[2] In particular: the canton of Bern (General Conditions of the Canton of Bern for Information Security and Data Protection in the Provision of IT Services); and the canton of Zurich (Allgemeine Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen)

2.2.2.2 Processing in accordance with the instructions and interests of the public authority

The data processor only processes the data in accordance with the instructions and in the interests of the public authority. Article 10a (1)(a) of the FADP as well as the various cantonal laws contain provisions stipulating that data may be processed only in the manner in which the public entity would itself be entitled to do so.

The Microsoft Privacy Statement (Data Protection Addendum, DPA)[3] includes these provisions. As the data processor, Microsoft will process Customer Data (and Personal Data, in particular) only in accordance with the customer's documented instructions and the Microsoft Privacy Statement in order to (a) provide online services to the customer and (b) protect its lawful business operations involved in the deployment of these online services. The agreements signed with the customer, the product and usage documentation, and the configuration of the Online Service features collectively constitute the complete and final instructions that the customer provides to Microsoft to process its data.

In particular, customer data will not be used for advertising, market research or profiling purposes.

2.2.2.3 Involvement of other data processors

In the paragraph relating to the instructions and controls in the event of subprocessing, the DPA explains how Microsoft proceeds with subprocessors and informs customers, in particular, of the changes that have occurred concerning such subprocessors. This paragraph describes the requirements that Microsoft imposes on subprocessors and clarifies that it is Microsoft's responsibility to ensure that its subprocessors comply with all of the requirements specified in the DPA.

The Microsoft Trust Center[4] manages the list, also indicating the services that list members provide, the location of their headquarters, and the scope and conditions of their access to customer data: http://aka.ms/mscloudsubprocessors.

In critical online services, neither Microsoft nor its subprocessors have ongoing administrative access to customer data or their solutions. Microsoft Cloud works with "Zero standing ADMIN," also called "Least Privilege," where administrative access is controlled by an authentication procedure (so-called "Lockbox"): if, for example, a customer calls Microsoft Support, the person in charge of the customer's case will then be granted privileges (perhaps allowing limited access to the customer's data). The grant of administrative access must go through multiple channels, time-boxes and a full audit process - and if the customer wants, the process can also include the customer's final approval through an extended "Lockbox" process, called "Customer Lockbox" (see chapter 4.11).

2.2.2.4 Data Security

In the case of outsourcing IT or data processing services, federal and cantonal legislation regarding information security and data protection generally require that the service provider guarantee sufficient data security. Most cantonal regulations do not define concrete protection measures but establish principles regarding the protective objectives to be guaranteed (**confidentiality, availability and integrity**). These include protecting against the following risks:

– unauthorized or accidental destruction;

– Accidental loss;

– Technical failure;

– Tampering, theft or misuse;

– Unauthorized modification, copying, access or other processing.

Personal data must be protected against these risks through the use of **appropriate technical and organizational measures**.

[3] Microsoft Online Services Data Protection Addendum (DPA): https://aka.ms/dpa

[4] https://servicetrust.microsoft.com

Microsoft uses several types of encryption at different levels in its online services and has published extensive documentation and white papers on this subject. On one hand, different encryption is applied to the stored data ("data at rest") within the operating environments ("Volume Level") as well as on the individual data files, which makes it possible to exclude any physical access to the data. Encryption protection can be further complemented by customer-managed keys, also called BYOK (Bring Your Own Key). Microsoft also applies encryption techniques to the transmission of data ("data in-transit"). In addition, Microsoft Online Services provides various other means for cloud customers themselves to apply and manage certain encryption techniques.

Using the Microsoft Trust Center[5] and the Security & Compliance Center service certification[6], cloud customers can directly and at any time view certification and audit reports along with other comprehensive information about data storage locations, cloud customer data access options, security measures and data protection. The cloud customer can therefore at any time get an idea of how Microsoft fulfills its security obligations.

2.2.2.5 Cross-border processing

Federal and cantonal data protection laws impose special requirements when personal data processed in cloud environments is transferred abroad or accessed from abroad.

In general, outsourcing to a country that applies the same level of data protection as Switzerland does not require any additional measures. This is particularly the case for all EU/EEA countries.

For SaaS online services for Swiss customers, by default Microsoft uses data centers in the Swiss region and sometimes in the European region (data centers in Ireland, Austria, Finland and the Netherlands). The customer data is stored in these data centers. The specific data retention locations can be viewed for each online service using the relevant Security & Compliance Center service certification[7].

The actual deployment of Microsoft Online Services or their individual configuration by the customer may, in some cases, require that certain customer data be made accessible to Microsoft employees or subprocessors who are located outside of the primary data storage region. Similarly, the Microsoft employees most skilled in resolving specific service issues may also be located outside of the primary data storage region and need online access to the systems or data in order to resolve the problem.

In accordance with its privacy statement applicable to online services, Microsoft is therefore fundamentally entitled to transfer, store and process the data of its cloud customers in other countries where Microsoft, its affiliates or subprocessors have installations (including in the United States). For all personal data originating from Switzerland, Microsoft hereby agrees to at all times comply with the requirements of Swiss data protection laws in terms of the collection, use, transfer, retention and other processing of such data.

---

[5] https://www.microsoft.com/en-us/trust-center

[6] https://docs.microsoft.com/en-us/microsoft-365/compliance/service-assurance?view=o365-worldwide

[7] https://docs.microsoft.com/en-us/microsoft-365/compliance/service-assurance?view=o365-worldwide

In the case of customer data, professional services data and personal data from the EU/EEA and Switzerland that would be transferred to so-called unsafe third countries, Microsoft has entered into so-called standard (Processor-to-Processor) contractual clauses between Microsoft Ireland Operations Ltd. and Microsoft Corp. USA. For exports of data from Switzerland, these standard contractual clauses have been adapted to Swiss conditions in accordance with the Federal Data Protection and Information Commissioner (FDPIC) recommendations.

On May 6, 2021, Microsoft announced with its "EU Data Boundary" plan that for its core online services: Azure, Microsoft 365, Dynamics 365 and Power Platform, critical customer data will be processed and stored in Europe and support provided from the European area.[8] This plan should be available at the end of 2022.

Microsoft will also not share customer data with law enforcement authorities, unless required by law. If law enforcement authorities contact Microsoft to request customer data, Microsoft will attempt to refer them to the customer for a direct request. If required to disclose or provide access to data to law enforcement authorities, Microsoft will immediately notify the customer and provide the customer with a copy of such request, unless prohibited by law. Microsoft takes a fundamental and thorough approach when responding to formal requests for access to the customer data in its possession.[9]

Microsoft publishes the Law Enforcement Request Report every six months to provide transparency on the number and nature of these incidents.[10] These reports are public and can be used for risk assessments. Microsoft interacts on a daily basis with customers and governments around the world to actively participate in establishing the international regulatory framework governing these issues. As a guideline, Microsoft has published six principles that also build on our ongoing efforts to protect our customers' data and enhance the protection of their data.[11] According to Microsoft, these principles represent universal rights and minimum baseline requirements, which, in our digital age, should govern the access to data by law enforcement authorities. While the application of these principles may vary from one country to another, the fundamental principles of control, checks and balances, accountability and transparency should nevertheless be maintained.

2.2.2.6 Public authority access to data

Microsoft firmly believes that customers have the right to be protected by their own laws. Microsoft takes a disciplined and principled approach to responding to law enforcement requests for the customer data in its control.[12] Here are the primary guidelines that Microsoft follows in all of its services:

- Microsoft does not provide any government with direct and unfettered access to our customers' data, and does not provide any government with our encryption keys or the ability to break our encryption.
- If a government wants customer data, it must follow the applicable legal procedures. It must serve us with a warrant or court order for content data, or a subpoena for subscriber information or other noncontent data.
- All requests must target specific accounts and identifiers.
- Microsoft's legal compliance team reviews all requests to ensure they are valid, rejects those that are not valid, and only provides the data specified.
- Following the Schrems II judgment, Microsoft has undertaken to legally challenge official requests from third parties[13].

Part of Microsoft's work on government requests includes publishing the "Law Enforcement Request Report" every six months,[14] which intends to guarantee transparency on the number and nature of these incidents.

[8] https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/

[9] The procedure is described in detail here: https://aka.ms/mslerh

[10] View here: https://aka.ms/mslerr

[11] "Six Principles for International Agreements Governing Law Enforcement Access to Data": https://aka.ms/MS6dataaccessPrinciples

[12] The procedure is described in detail here: https://aka.ms/mslerh

[13] See also: https://blogs.microsoft.com/on-the-issues/2020/11/19/defending-your-data-edpb-gdpr/

[14] https://aka.ms/mslerr

To assess the risk of law enforcement access to data, consider the actual number of incidents reported in the Microsoft Law Enforcement Request Reports, which are available using the link above. More than 90% of requests from authorities relate to private customer data, such as Hotmail or Skype.

According to these statistics...

– ... it is unlikely that a specific customer entreprise is targeted by such a request,

– ... it is even less likely that such request will NOT be rejected or redirected and

– ... it is even more unlikely that such a request for data stored outside of the country of origin of the request will NOT be rejected or redirected.

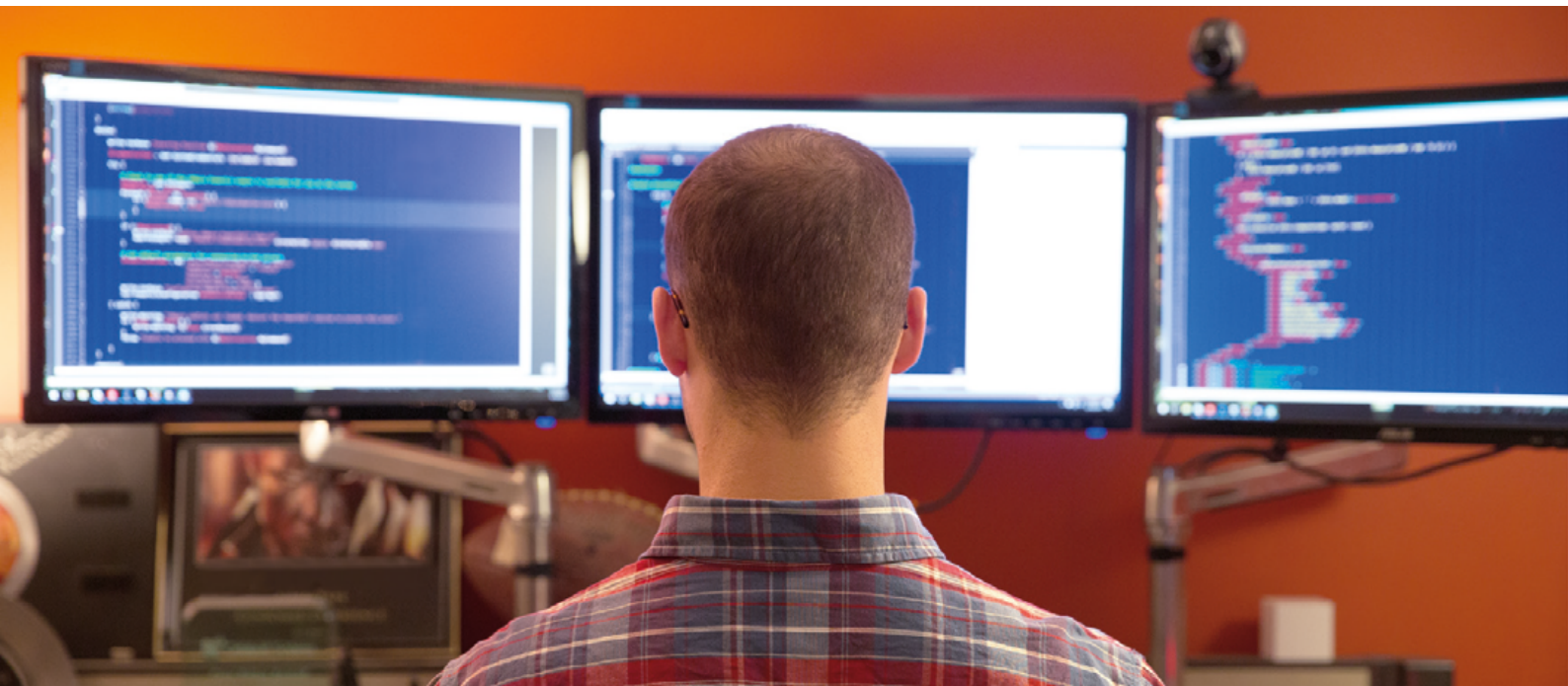
Based on these reports and considering Microsoft's fundamental process and history of protecting the privacy rights of its customers, customers should be able to assess the risks and see that the likelihood (and therefore total risk) of requests from law enforcement authorities of third countries is absolutely minimal or almost non-existent.

It should also be noted that the difference in the figures between requests for personal accounts and those for business accounts also reflects the official recommendations[15] of the Computer Crime and Intellectual Property Section of the United States Department of Justice. According to these recommendations, prosecutors who wish to access a company's data are advised to approach them directly and not try to go through cloud service providers, to the extent that this is feasible and does not otherwise compromise the investigation.

2.2.2.7 Sensitive data

In the case of very specific information that, for reasons of public interest, should not fall into the hands of third parties because it affects, for example, the security of critical community infrastructure, an explicit or implicit restriction could be applied on cloud service usage. In this regard, this community would be required to use information classifications to delimit the data that is not to be included in a cloud project. It is necessary to specifically plan these aspects on a case-by-case basis and take the appropriate measures for this purpose. The following chapter examines the basic principles in detail.

[15] https://aka.ms/USDoJSeekingEnterpriseData



2.3 SWISS INFORMATION PROTECTION ORDINANCE (IPO)

The *Swiss Information Protection Ordinance* (IPO, 2015)[16] regulates the protection of information of the Confederation and armed forces as necessary in the interests of the country. In particular, it determines the classification and processing of this information. In essence, this ordinance defines the classification levels to be attributed to the information according to the degree of required protection and then proposes the appropriate measures. It defines the following 3 classification levels: SECRET, CONFIDENTIAL, INTERNAL.

The table below summarizes all of the electronic information processing measures applicable by level.

Tier / Processing procedure	**INTERNAL (RESTRICTED[17])**	**CONFIDENTIAL**	**SECRET**
Classification statement (label)	Mark every page with: "INTERNAL"	Mark every page with: "CONFIDENTIAL"	Mark every page with: "SECRET"
Backup and retention	Compulsory protection	Encrypted on workplace systems or encrypted on removable data carriers	Only on authorized resources or in encrypted form on workplace systems or on removable data carriers
Data transmission	Protected transfer pathway (e.g., federal network)	Encryption or protected transfer pathway	Encryption or protected transfer pathway
Processing with IT applications	Permitted	Only with resources authorized by the Coordination Agency (exception: armed forces) and with the use of security software that satisfies Swiss federal standards	Only with resources authorized by the Coordination Agency and with the use of security software that satisfies Swiss federal standards
Removal from permanent location	Permitted	Permitted in restricted cases	Permitted in restricted cases
Withdrawal and withdrawal obligation	None	Compulsory	Compulsory
Destruction or erasure	Permitted in restricted cases	Permitted in restricted cases	Only by the author

Table 1 – Matrix of classification levels and measures according to the IPO

This ordinance also applies to organizations and persons under public and private law and to federal and cantonal courts that handle classified information, to the extent that this is provided for under federal law or by agreement.

[16] https://www.fedlex.admin.ch/eli/cc/2007/414/en

[17] Information classified as "RESTRICTED" or an equivalent degree and which comes from abroad is processed as information classified as "INTERNAL."

3 CONTROL OBJECTIVES AND RISKS

As in other areas, usage of the cloud is not subject to laws or rules that inherently prohibit or authorize its use. Data protection officers of public entities must therefore conduct risk analysis, taking account of applicable legislation, the type of data, the type of processing and possible protection and control measures, in order to decide whether transition to the cloud is possible or not.

Before choosing the appropriate measures, it is important to know the classification of data and information and consult the documentation on this subject (see chapter 2.3). This classification also serves as a basis for the configuration and control of the technologies and the means applied for the implementation of the measures. Any organization should provide protective measures adapted to each category of data based on the Ordinance provisions concerning the protection of information (see chapter 2.3). These safeguards, which include contractual, organizational, and technical safeguards, could be applied by a company as follows:

- **Secret data**
  First, the secret data is not saved in the cloud but on premise. To fully take advantage of Azure's security features, the data is stored on an Azure Stack HCI managed by Azure Arc.
- **Confidential data**
  The storage of confidential data in the cloud is permissible as encrypted. In this case, Azure Information Protection (AIP) is the solution to choose, either with its own key (BYOK) or with two keys – one in Azure and another on premise with the customer (Double Key Encryption).

The following chapters will not cover the measures to be applied at each classification level but rather propose the control objectives and the possible risks that are to be taken into consideration and addressed in the Public Cloud decision-making process. The measures to be adopted will then depend on the nature, structure and information of the data.

3.1 CONTROL OBJECTIVES

The widely known "Information Security Triad" model can be used as a basis to classify the risks and appropriate measures. It focuses on the three main components of information security **C**onfidentiality, **I**ntegrity and **A**vailability. Its primary aim is to achieve the following general control objectives by answering the associated questions.

ID	Domain	Purpose and description	Basics
OC1	C	**Access rights** Is the data under the responsibility of the data processor sufficiently protected against unauthorized physical access (e.g. protection of confidentiality)?	Information security best practices (e.g. minimum IT standard of NESA) | Art. 7 and Art. 10a para. 2 DPL, Art. 8 and Art. 9 para. 1 let. a ODPL | Art. 8 para. 1–2 and Art. 9 para. 2 DPL rev.
OC2	C	**Access control** Are electronic access rights sufficiently regulated?	Information security best practices (e.g. minimum IT standard of NESA) | Art. 7 and Art. 10a para. 2 DPL, Art. 8 and Art. 9 para. 1 let. g ODPL | Art. 8 para. 1–2 and Art. 9 para. 2 DPL rev.
OC3	C	**Usage controls** Is the monitoring of persons having permanent or temporary access to data sufficient to minimize the risk of unauthorized data usage and enable the tracing of breaches?	Information security best practices (e.g. minimum IT standard of NESA) | Art. 7 and Art. 10a para. 2 DPL, Art. 8 and Art. 9 para. 1 let. d and h NESA | Art. 8 para. 1–2 and Art. 9 para. 2 DPL rev.

OC4	C	**Erasure control** Is it guaranteed that the subprocessor delete the data at the end of the outsourcing contract?	Art. 10a para. 1 let. a DPL | Art. 9 para. 1 let. a DPL rev.
OC5	I	**Integrity control** What provisions have been implemented to prevent the data processor or other third parties from manipulating the data?	Information security best practices | Art. 7 and Art. 10a para. 2 DPL | Art. 8 para. 1–2 and Art. 9 para. 2 DPL rev.
OC6	A	**Availability check** How is data availability ensured?	Information security best practices (e.g. minimum IT standard of NESA) | Art. 7 and Art. 10a para. 2 DPL | Art. 8 para. 1–2 and Art. 9 para. 2 DPL rev.
OC7	A	**Data restoration** How is it guaranteed that data can be restored in the event of loss or error?	Information security best practices | Art. 10a para. 1 let. a DPL | Art. 9 para. 1 let. a DPL rev.

Table 2 – Information security control objectives

3.2 RISK ANALYSIS

The list of risks presented below can be evaluated by public authority decision-makers and used for decision-making. The risks are accompanied by the contractual, organizational and technical measures that arise from them and are explained in the following chapter. This list can be expanded in the event of additional regulations (cantonal or municipal, for example). The risks arise from the control objectives set forth in chapter 3.1 and are also classified according to the **C**-**I**-**A** general method. Some risks refer only to the legal or regulatory basis (**REG**) because they can only be indirectly assigned to one of the three information security areas. The risks are deliberately focused on the relationship between the customer and the data processor. In addition to the contractual and organizational measures affecting the relationship with its data processor, the customer also has the option in most areas of providing itself with other technical protection and security measures that respond to the specific risk. This may involve measures minimizing the risks incurred with the data processor or with potential unauthorized third parties. Each risk requires answering this additional question: "As a customer, how and with what additional measures to those of the data processor can and should I address this risk?"

The table of risks presented below also proposes corresponding measures. These are the measures taken by the data processor (agreements, documentation) and those that the customer can take.

ID	Domain (C-I-A), REGulation	Risk	ID of the measures	Impact of the risk after the measure	Probability of occurrence of the risk	Risk assessment	Residual risk mitigated?
R1	REG	**Subprocessor** Is it guaranteed that the data processor inform the customer of the use of subprocessors and grants the customer a right of opposition in the event of the replacement or use of new ones (Art. 9 para. 3 DPL rev.)? Are the subprocessors of the data processor subject to the same legal and regulatory basis as the data processor?	M15				
R2	REG	**Insufficient data security** Is it guaranteed that the data processor sufficiently protect the confidentiality, integrity and availability of the customer's personal data (Art. 10a, para. 2, DPL | Art. 9, para. 2, DPL rev.)? Is the performance of an audit to verify compliance with applicable security procedures and guidelines guaranteed and clearly documented?	M8 M10 M15 M16				
R3	REG	**Unreported information security breach** Is it guaranteed that the data processor will notify the customer of information security breaches (Art. 10a para. 2 DPL | Art. 9 para. 2 and Art. 24 para. 3 DPL rev.)? Does the data processor monitor the services for any security breaches and does it proactively perform optimizations?	M7 M15				
R4	REG	**Specific purposes of the data processor** Is it guaranteed that the data processor will only use the personal data processed on behalf of and for the purposes of the customer and not for its own purposes (Art. 10a para. 1 let. a DPL | Art. 9 para. 1 let. a DPL rev.)? How is data ownership regulated? How are roles and responsibilities divided between the customer and the data processor?	M15 M16				
R5	REG	**Cross-border communication** Have adequate safeguards (such as European contractual clauses, for example) been implemented to ensure the appropriate protection of personal data transmitted to countries that do not offer a sufficient level of data protection (Art. 6 and Art. 10a para. 1 let. a DPL | Art. 16 and Art. 9 para. 1 let. a DPL rev.)?	M15				
R6	C REG	**Disclosure of secrets** Is information subject to professional or official secrecy sufficiently protected against access in plain text by the subcontractor or third parties (Art. 320 PC, Art. 321 PC)? Is the data processing by the data processor subject to an adequate confidentiality obligation?	M2 M3 M4 M11 M12 M13 M15 M16				
R7	REG	**Public authority data access** Does the data processor provide sufficient oversight over its processes and guidelines regarding the State's access to data to allow the customer to make an informed decision (best practice)?	M15 M16				

R8	CIA REG	**Lack of governance** Has the data processor provided the customer with sufficient insight into its own internal control system (ICS) (best practice)? Is the performance of an audit to verify compliance with applicable security procedures and guidelines guaranteed and clearly documented?	M1 M10 M15 M16
R9	I REG	**Insufficient reports** Does the data processor provide sufficient reporting on outsourced activities and services (best practice)? Is the performance of an audit to verify compliance with applicable security procedures and guidelines guaranteed and clearly documented?	M7 M15 M16
R10	C	**Unauthorized access to the data storage location (OC1)** Does the data processor guarantee a certain transparency regarding the technical and organizational measures that it uses to protect customer data against unauthorized and physical access, as well as regarding encryption during transfer, protection against malware, confidentiality, authentication and the operational guidelines applicable to its personnel?	M4 M5 M6 M15 M16
R11	C	**Unauthorized access to data content (OC2)** Is the data processor able to state policies on access to components and data and show that it has implemented sufficient security procedures and policies? Are there procedures to ensure the accessibility of data after failures?	M5 M6 M15 M16
R12	C, I	**Unauthorized use of data (OC3)** Can the data processor guarantee and demonstrate that it either has no access to the customer's data or can only view such data in the proper course of its subcontracting duties? Is there any logging of the data access events? Does the data processor have confidentiality obligations applicable to its necessary duties?	M7 M15
R13	C	**Improper data erasure (OC4)** Does the data processor have clear guidelines on how to handle the termination of a subscription or the deletion of data by the customer? Are hardware components properly disposed of according to applicable industry standards? Is the data portable? Is a contractual right of oversight on this topic guaranteed?	M9 M15
R14	I	**Data breach (OC5)** Does the data processor ensure that its personnel are trained in the required security procedures and guidelines (e.g. administration session or password management) and actively enforce them?	M15 M16
R15	A	**Reduced availability and data recovery (OC6 & OC7)** Does the data processor make available, for each service, documentation concerning the SLA and the resulting guarantees? Has the data processor implemented business activity monitoring? Is it clear what will happen if the data processor decides to terminate certain services? Are platform-dependent restoration procedures and their verification implemented? Are the customer's responsibilities clearly defined in this context?	M9 M15 M16

Table 3 – Risk analysis based on legislation and the fundamentals of information security

4 MEASURES AND DESCRIPTION OF THE COMPONENTS

This chapter proposes and explains the possible measures to counter the risks listed above. These measures are not listed in order of priority.

ID of the measures	Domain	Measure	Type of measure
M1	C, I, A	ISO 27001	Organizational, contractual
M2	C, I, A	Azure Purview	Technical, organizational
M3	C, I, A	Azure Resource Tags	Technical, organizational
M4	C, I	Azure Key Vault	Technical
M5	C	Azure IAM (RBAC)	Technical, organizational
M6	C, I, A	Azure Policies	Technical, organizational
M7	A	Azure Monitor	Technical
M8	C	GDPR Compliance Manager	Technical, organizational, contractual
M9	C	Azure Data Subject Requests for GDPR	Technical, organizational
M10	C, I, A	MPSCD training	Organizational
M11	C	Customer Lockbox for Azure	Technical, organizational
M12	C, I, A	Azure Stack Hub	Technical, organizational
M13	C, I, A	Azure Stack HCI	Technical, organizational
M14	C, I, A	Azure Arc	Technical, organizational
M15	C	Agreements	Contractual
M16	C, I, A	Shared Responsibility Model	Organizational, contractual

Table 4 – List of measures

4.1 M1 – AZURE BLUEPRINT – ISO 27001

Azure Blueprints are templates that group resources, policies and permissions that are applicable and reusable as a set to deploy one or more standard-based environments in Azure.

The base model used for the Swiss Public Sector Cloud Design is an already existing blueprint based on the ISO 27001 security standard and to which specific extensions were added to meet identified needs.

This solution allows identified risks to be addressed through the following objectives:

- Policy: limiting the backup of cloud resources and data processing to the Swiss or European Azure region
- Policy: application of secure or encrypted transmission protocols (TLS/SSL) on the communication of cloud resources
- Policy: application of activity log collection for all resources and services.

– Permissions: creation and assignment of access rights to resources and services ensuring a differentiated and role-based access control on the components and functions of the Azure environment

– Resource: creation of a Key Vault for the secure storage of encryption keys

– Resource: creation of a Log Analytics Workspace for the storage and possible evaluation of activity logs

Additional components can be added to the blueprint at any time or individual measures can be added to complement the blueprint.

Figure 1 – Blueprint ISO 27001

4.2 M2 – AZURE PURVIEW

The Azure Purview tool is used for the universal and centralized collection of all data stored in the cloud (not only Azure) and on-premise resources, as well. The tool makes it possible to obtain a holistic map of all the information in metadata form. The classification and origin of the data are the subject of special attention to enable evaluation of the data estate, to take possibly necessary measures or simply to find information.

The information index (data catalog) is automatically created from the regular scans of known resources: the standardized and user-defined classification rules that are used then serve as filters during the data search. The classification criteria and a glossary facilitate the identification and localization of information.

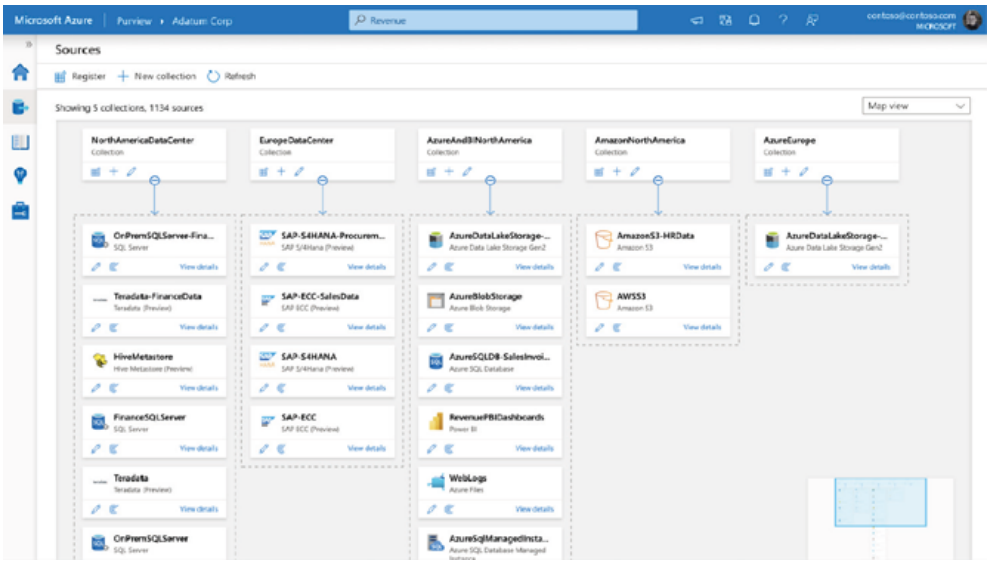


Figure 2 – Azure Purview

The standardized Apache Atlas interface allows metadata to be imported into the catalog from other sources.

Azure Purview is strongly recommended for the classification and indexing of data stored in Azure and as a monitoring tool for data protection officers.

This solution allows identified risks to be addressed through the following objectives:

– identification and management of confidential data.

4.3 M3 – AZURE RESOURCES TAGS

Resources Tags are another universal way to classify resources and their stored data. These tags represent freely definable meta information that can be applied at different levels of the controlled Azure infrastructure and can themselves be evaluated for different purposes. Azure Resource Tags are a Key Value Pair.

This solution allows identified risks to be addressed through the following objectives:

– Identification and management of confidential data.

4.4 M4 – AZURE KEY VAULT

The Azure platform is always encrypted by Microsoft and you manage the keys. Azure Key Vault is a PaaS service to generate customer-specific (a-/symmetric) keys that are dedicated to encrypting their data. Explicit key access rights that are granted to resource service accounts, such as storage accounts or Azure SQL DB, ensure that no human interaction is required with encryption keys and certificates, and that encryption and decryption are done transparently.

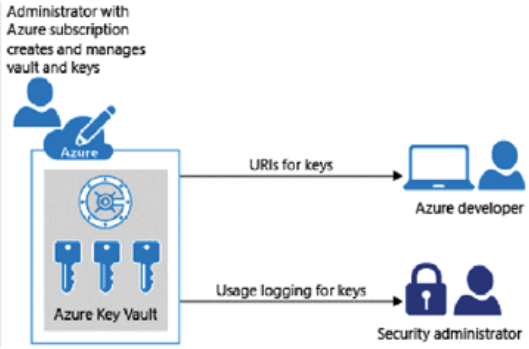


Figure 3 – Azure Key Vault

Encryption keys and certificates are stored in software instances of Key Vault that are controlled by the customer. If the storage of encryption keys needs to be done in dedicated hardware security modules (HSMs) or even in its own on-premise HSM, Key Vault Managed HSM can take care of it.

If any of the following requirements apply to your organization, you can protect your customer content using Key Vault with or without Managed HSM:

– You must be the only one who can decipher the protected content

– You do not want Microsoft to have access to very sensitive data

– You are required by law to keep the encryption keys within a geographic boundary

This solution allows identified risks to be addressed through the following objectives:

– Encryption of sensitive data.

4.5 M5 – AZURE IAM (ROLE BASED ACCESS CONTROL RBAC)

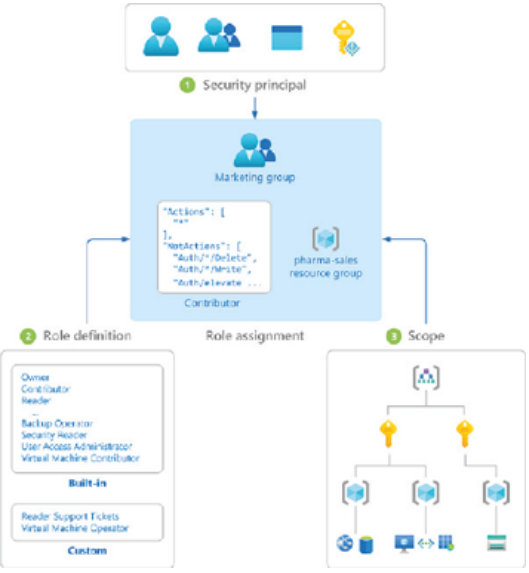


Figure 4 – Azure IAM (RBAC)

The segregation of tasks and access control to the Azure platform and its service and application resources are provided by the integrated, role-based authorization system, with Azure AD performing the prior authentication of identities. Azure offers many predefined roles that determine access rights to platform resources and elements and can be assigned to the different identity types.

However, the authorization system enables the creation of user-specific role definitions and assignments if the standard roles offered are not sufficient.

This solution allows identified risks to be addressed through the following objectives:

– Protection of access to resources.

4.6 M6 – AZURE POLICIES

Azure Policies are policies that regulate Azure infrastructure to verify or even enforce large-scale organizational requirements. The dashboards allow you to get a consolidated overview of compliance and also focus on compliance by resource or policy.

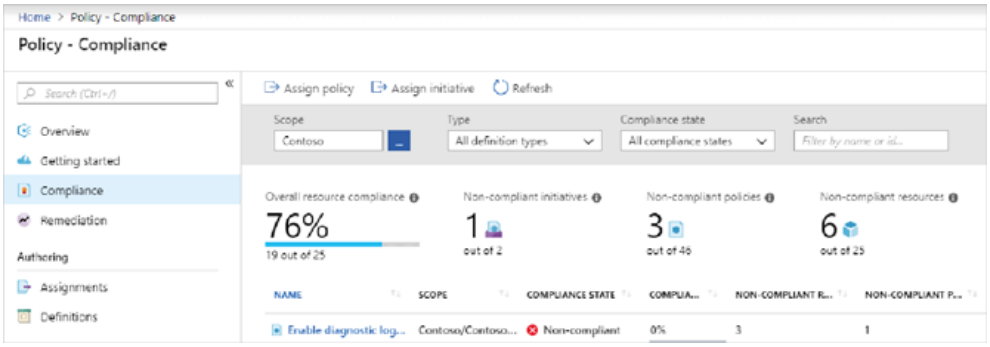


Figure 5 – Azure Policies

These policies are great tools to enforce or control the following requirements, in particular:

– Limiting the deployment of resources to authorized Azure regions (e.g. Switzerland, EU);

– Required use of encrypted data transmission with predefined certificates;

– Enforced application of data encryption using authorized encryption algorithms;

– Forced consolidation of all activity logs.

Many predefined policies are offered here that can be used directly and supplemented by user-specific rules, as necessary.

This solution allows identified risks to be addressed through the following objectives:

– Limiting the backup of cloud resources and data processing to the Swiss or European Azure region;

– Application of secure or encrypted transmission protocols (TLS/SSL) on the communication of cloud resources;

– Application of activity log collection for all resources and services.

4.7 M7 – AZURE MONITOR

Azure Monitor brings together all of the means to monitor the availability, performance and events of the Azure platform and the services and resources used. It allows you to configure alerts based on thresholds and events that will trigger additional notifications (e.g. email, SMS) or automations in order to ensure service continuity.

Workbooks allows you to create Monitoring Dashboards with visual indicators concerning availability and performance as well as event logs.

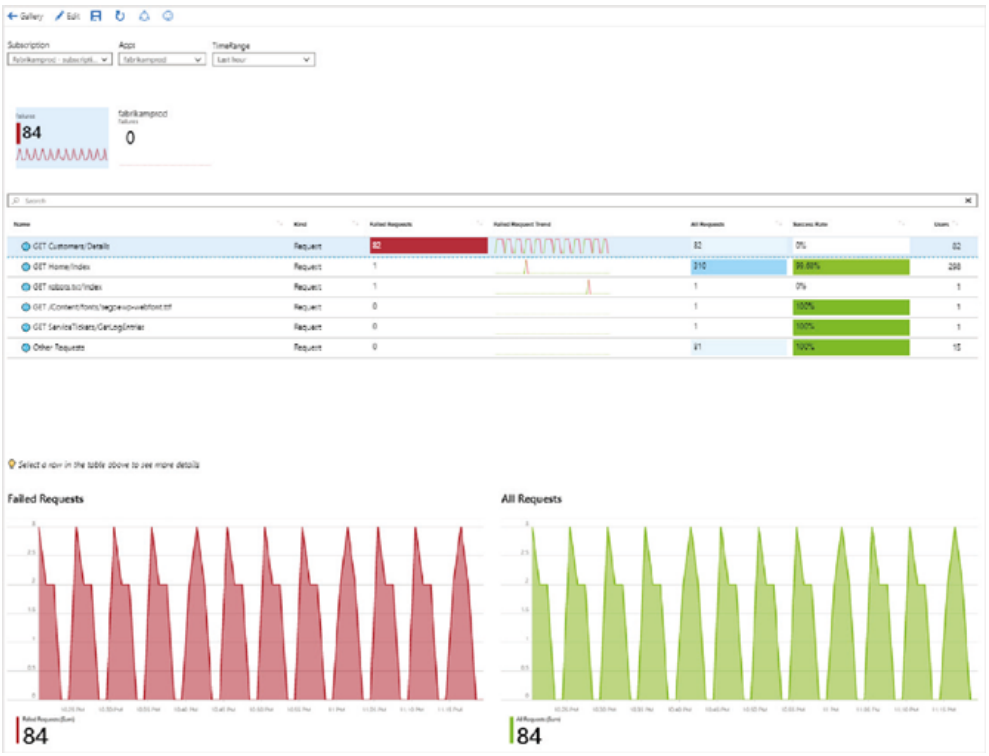


Figure 6 – Azure Monitor

This solution allows identified risks to be addressed through the following objectives:

– Providing an overview of resource availability;

– Alerts in the event of possible malfunctions and threats.

4.8 M8 – MICROSOFT GDPR COMPLIANCE MANAGER

Compliance Manager is a tool to monitor and verify your institution's compliance and Azure implementation with the European Union's General Data Protection Regulation.

GDPR Compliance Manager offers you additional features:

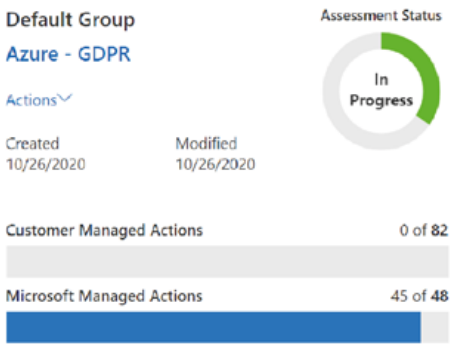


Figure 7 –
Microsoft GDPR Compliance Manager

– Combination of information that Microsoft makes available to auditors and regulators;

– Attribution of compliance activities and their tracking and recording;

– Assessment to help you understand and prioritize the controls intended to minimize risks;

– A secure repository for documentation and other artifacts;

– Creation of detailed reports that can be provided to auditors, supervisory authorities or other stakeholders.

This solution allows identified risks to be addressed through the following objectives:

– Guarantee of GDPR compliance.

4.9 M9 – AZURE DATA SUBJECT REQUESTS FOR GDPR

The European Union's General Data Protection Regulation (GDPR) gives every data subject the right to influence the personal data that is collected about him or her by an organization. The GDPR grants data subjects certain rights over their personal data, in particular, by allowing them to request copies of such data as well as its correction, processing restriction, deletion or provision in electronic format with a view to transfer to another data controller or another data processor. A formal request from a data subject asking the data controller to take action on their personal data is called a Data Subject Request or DSR.

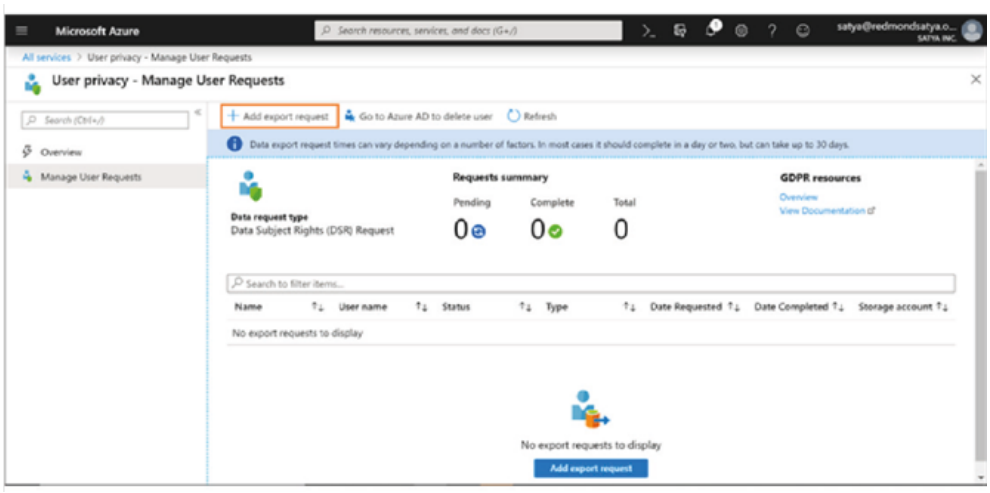


Figure 8 – Azure Data Subject Requests for GDPR

The Azure Data Subject Requests for GDPR tool helps process data subject requests in accordance with the GDPR.

This solution allows identified risks to be addressed through the following objectives:

– Management (access, restitution and deletion) of relevant data within the meaning of the GDPR.

4.10 M10 – TRAINING FOR MICROSOFT PUBLIC SECTOR CLOUD DESIGN

To ensure the effective use of Azure as a cloud platform, its components and the concepts presented here, it is also essential that the personnel tasked with its use undergo training.

– Some members of the Microsoft Partner Network offer an introduction to Microsoft Cloud Design.

Basics	Technology	Operation
– Cloud Design Introduction – Swiss Data Protection Act (DPA) – Swiss Information Protection Ordinance (IPO) – Information Security (ISO 27001) – Classification of Information	– Blueprints (templates) – Purview (data catalog) – Policies – Key Vault (encryption) – Monitor – Customer Lockbox	– Blueprint Deployment – Compliance Analysis – Policy Creation – Environment Setup – Continuous Verification – Monitoring

Figure 9 – Training in Microsoft Public Sector Cloud Design

This solution allows identified risks to be addressed through the following objectives:

– Prevention of handling errors;

– Business continuity assurance;

– Better understanding of the technologies, risks and opportunities for IT departments.

4.11 M11 – CUSTOMER LOCKBOX FOR AZURE

Customer Lockbox for Microsoft Azure allows you as a customer to review and approve/reject a request to access your data from Microsoft. It is used in cases where a Microsoft technician needs access to customer data during a support request.

In particular, you can assess whether the information to be transmitted when requesting assistance is confidential or not and whether or not it can be viewed.

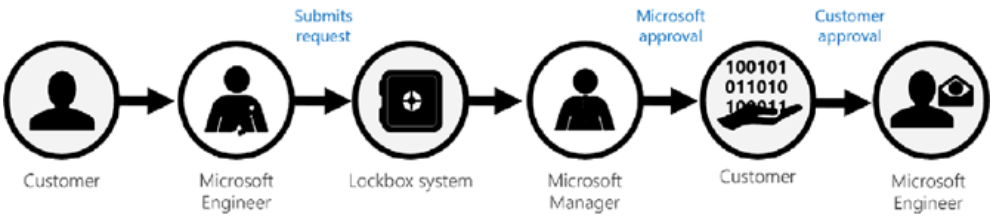


Figure 10 – Customer Lockbox

This solution allows identified risks to be addressed through the following objectives:

– Maintenance of personal data confidentiality.

4.12 M12 – AZURE STACK HUB

Azure Stack Hub is your own private Azure cloud that can operate fully or partially disconnected from the Internet. Azure Stack Hub is a part of the Azure Stack portfolio that is an extension of Azure allowing you to run applications in an on-premise environment and deploy Azure services in your data center. Many businesses undergoing digital transformation find that they can accelerate this process by taking advantage of public cloud services to build modern architectures and update their applications. However, some workloads must remain on-premise - partly due to different technical and legal requirements. Azure Stack Hub allows you, for example, to store sensitive and classified data.

Figure 11 – Azure Stack Hub

This solution allows identified risks to be addressed through the following objectives:

– Data storage in your own data centers.

4.13 M13 – AZURE STACK HCI

Azure Stack HCI serves the same purpose as Azure Stack Hub: To use the data on-premise that must not migrate to the cloud.

Azure Stack HCI is a standards-based, hyperconverged virtualization platform that has been developed and certified by hardware manufacturers and Microsoft. It allows virtual servers to be operated on the platform and provides the following infrastructure services:

– Azure Stack HCI operating system

– Hardware verified by an OEM partner

– Azure hybrid services

– Windows Admin Center

– Virtual machines on Microsoft Hyper-V

– Memory virtualized directly to Storage Spaces

– SDN-based virtualized network with (optional) network controller

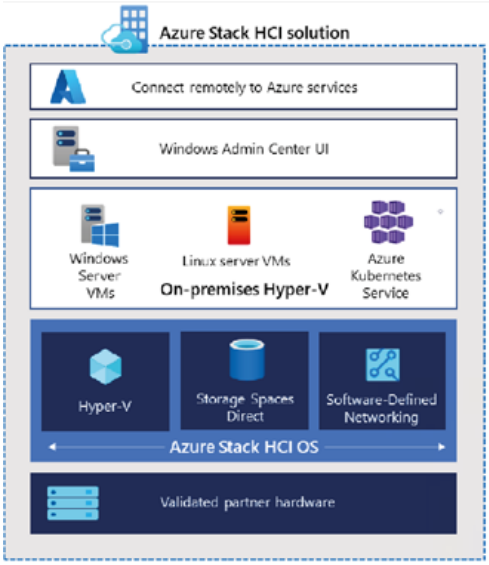


Figure 12 – Azure HCI

Azure Stack HCI enables the use of the following Azure services:

- Monitoring: View all of your Azure Stack HCI clusters together by grouping and referencing them by resource groups.
- Invoicing: Pay for Azure Stack HCI through your Azure subscription.

You can also use other Azure hybrid services:

- Azure Site Recovery, to provide a high availability and disaster recovery service (Disaster-Recovery-as-a-Service, DRaaS)
- Azure Monitor, a hub where you can monitor the activity of your applications, networks and infrastructure using advanced AI analytics
- Cloud Witness, to use Azure as an arbitration point
- Azure Backup, to protect data through storage in other locations and against ransomware
- Azure-Update Management, to assess and deploy updates to Windows VMs running in Azure and on-premise
- Azure-Network Adapter, to connect local resources to your Azure-hosted virtual machines using a Point-to-Site-VPN
- Azure-File Sync, to synchronize your data server with the cloud

This solution allows identified risks to be addressed through the following objectives:

- Data storage in your own data centers.

4.14 M14 – AZURE ARC

Azure Arc provides a consistent platform for various public clouds and the on-premise environment to simplify governance and management. Azure Arc allows you to perform the following:

- The entire environment can be managed through a centralized user interface thanks to the visualization in Azure Resource Manager of existing resources (resources from Azure, on-premise environment or other clouds)
- Management of VMs, Kubernetes clusters and databases, as if running in Azure
- Implementation of a consistent inventory, management, governance and security solution for servers in your entire environment
- Configuration of Azure VM extensions to use Azure management services to monitor, protect, and update your servers
- Consistent visualization of your resources compatible with Azure Arc through the use of Azure-Portal, Azure CLI, Azure PowerShell or Azure-REST-API

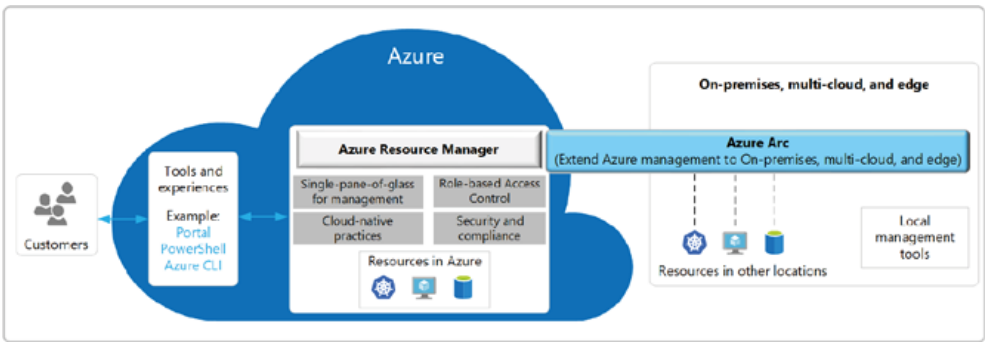


Figure 13 – Azure Arc

This solution allows identified risks to be addressed through the following objectives:

– identification and management of confidential data;

– Minimizing security vulnerabilities through updates and antivirus programs for cloud and on-premise workloads;

– Consistent governance for all of the resources used;

– Resource compliance ensured by centralized management.

4.15 M15 – AGREEMENTS

To better understand and appreciate Microsoft Cloud and thus better assess this control, it is essential to know the overall structure of Microsoft Cloud agreements, documentation, guides and, especially, its certifications and audit reports. The Microsoft Assurance Framework provides the necessary overview and serves as a guide for the audit process to be followed:

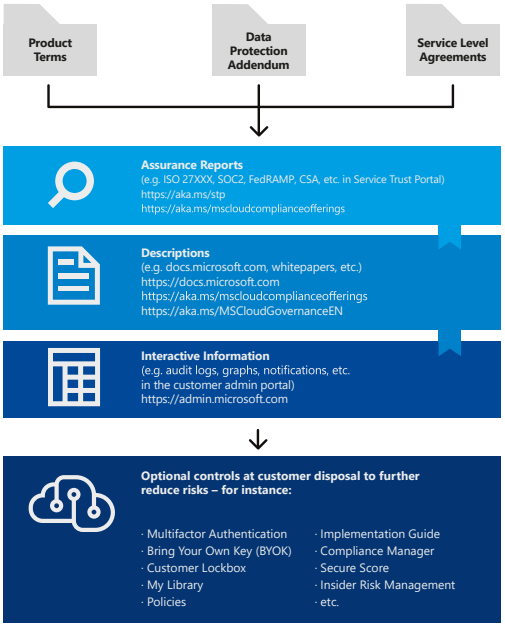


Figure 14 – Microsoft Assurance Framework

– The first level consists of the **agreements to be signed with Microsoft**, which include, in particular, the **License Terms** stipulating the data processing agreement (**Data Protection Addendum** for Microsoft Cloud).

– Microsoft's contractual obligations that are defined in the agreements are contained in the second level documents, the **Assurance Reports**. Customers can access all **third-party audit reports, certificates on compliance with standards, SOA,** etc.

– The third level includes more detailed descriptive documentation where Microsoft provides **instructions and descriptions** on a number of functions, features, processes and other topics. A series of **white papers** are also offered on the specific themes and sectors, such as this document.

– Finally, customers have access to up-to-date documentation and information on the use of Microsoft cloud services, which are available on a personalized cloud service management **portal**.

For all of these four levels, there are other functions, services and processes that can be implemented, depending on the customer. Their deployment is based on the overall risk assessment of the solution and data flows, and is part of a mitigation plan that responds to the identified risks that the customer wishes to mitigate. The figure in the upper right presents some of the most common measures that will be explained later in this document.

Microsoft Assurance Framework therefore plays an essential role in the development of the controls to be implemented by the customer. This interaction is represented in the following process model:

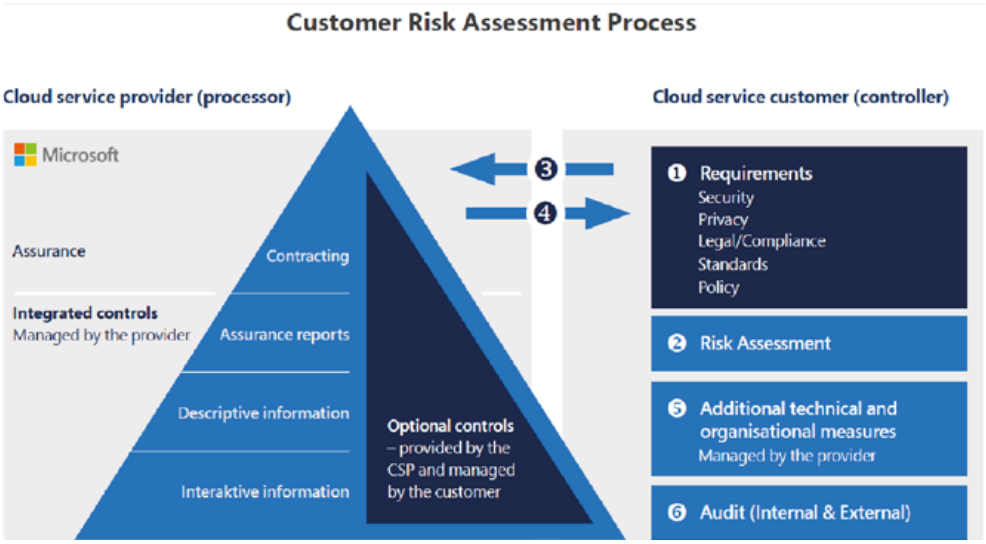


Figure 15 – Interaction between the Customer's Cloud Governance and Microsoft Assurance Framework

This solution allows identified risks to be addressed through the following objectives:

– Compliance assurance;

– Limitation of the risks through policies.

4.16 M16 – SHARED RESPONSIBILITY MODEL

The configuration or organization of the control, or the association and interaction of the various control instruments vary depending on the degree of integration of the cloud solutions involved. The same applies to the allocation of responsibilities and costs incurred when implementing the protection adapted to certain risks (data protection and security, in particular).

In a cloud environment, and unlike within on-premise IT infrastructure, both the customer and the cloud provider share responsibilities for implementing and monitoring IT application security controls. This situation evokes a classic outsourcing scenario. However, the ultimate responsibility for processed data always remains with the customer.

Modern cloud solutions are fundamentally based on a shared responsibility model. This model divides the responsibility between the customer and the cloud provider following a line of demarcation marked by virtualization, so that each party is primarily responsible for its side of the line.

Figure 16 – Shared Responsibility Model

With cloud solutions, the control function undergoes a certain evolution as its organizational/operational aspects gain in importance. In a cloud environment, a public authority, for example, has limited possibilities itself to implement technical measures against unauthorized access to data (since it is the cloud provider that provides the technology), and must therefore assume its responsibility through other appropriate measures. In addition to a careful assessment of the cloud provider, the public authority could fulfill its monitoring obligation by regularly monitoring the effectiveness of the data protection provided by the provider (for example, by continuously monitoring access and attempted access in the event logs).

To ensure the quality of the cloud provider's portion of the Shared Responsibility Model, Microsoft has performed numerous security, industry and national audits for Azure to obtain third-party Security Compliance certification in the operation of the cloud platform. The security standards applied are ISO and SOC, among others, the reports of which can be consulted in the Service Trust Portal[18].

This solution allows identified risks to be addressed through the following objectives:

– Distribution o**f responsibilities between the provider and customer;**

– **Risk evaluation assistanc**e.

[18] https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide

Microsoft

APPENDIX: CONTRACTUAL BASES AND IMPORTANT LINKS

The following table lists the primary sources of information in this document that are cited for the sake of transparency.

Document or subject	Links
Privacy Statement Landing Page	https://privacy.microsoft.com/en-us/privacystatement
Data Protection Addendum for Products and Services (DPA), September 2021	https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=1&year=2021
Universal License Terms for Online Services	https://www.microsoft.com/licensing/terms/product/ForOnlineServices
Microsoft Business and Services Agreement (MBSA)	https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4f5aA
Azure services technical documentation	https://docs.microsoft.com/en-us/
Microsoft Trust Center (Compliance & Security documentation)	https://www.microsoft.com/en-us/trust-center
SLA documentation of all Azure services	https://azure.microsoft.com/en-us/support/legal/sla/summary/

Table 5 – Compilation of important sources of information

Microsoft

Thank you
Danke
Grazie
Engraziel